Hans Opolka

Central simple algebras and Galois representations

Braunschweig : Institut für Analysis und Algebra, 2009

Veröffentlicht: 23.07.2009

http://www.digibib.tu-bs.de/?docid=00028816

CENTRAL SIMPLE ALGEBRAS AND GALOIS REPRESENTATIONS

Hans Opolka
TU Braunschweig
Institut für Analysis und Algebra
Pockelsstrasse 14
D - 38106 Braunschweig

e-mail: h.opolka@tu-bs.de

Abstract: This is a survey about connections between central simple algebras and Galois representations in the case of number fields

AMS Classification 2000: 12 A 80, 11 R 32, 11 R 34
Key words and phrases: Central simple algebras, Galois theory of number fields, Galois cohomology

§1. Regular crossed products and Galois representations

The connection between the theory of central simple algebras and Galois representations is based on a result of R. Brauer [B] which says that every such algebra is similar to a crossed product with a Galois 2-cocycle all of whose values are roots of unity. At first we describe the basic construction which leads to this connectionin, for details see also [$O3$] . Let k be a field, let $\overline{k}$ be a separable algebraic closure of k, and for every subextension k'/k of $\overline{k}/k$ let $G_{k'} = G(\overline{k}/k')$ denote the profinite Galois group of the extension $\overline{k}/k'$. Denote by μ_k the group of roots of unity in k and for every positive integer m let μ_m denote the group of m-th roots of unity in $\overline{k}$. It is well known that every associative finite dimensional central simple k-algebra $\mathfrak{A}$ (c.s. k-algebra for short) such that the characteristic of k does not divide the exponent of $\mathfrak{A}$ is similar to a crossed product $(K/k, c)$, where K/k is a finite Galois subextension of $\overline{k}/k$ - with Galois group $G = G(K/k)$ say - and where $c : G \times G \to \mu_K$ is a Galois $2-$cocycle, see [B], §6, Satz 10. Adopting a terminology from [B], §2, such a crossed product is called *regular.* It is also shown in [B] , §6, that $\mathfrak{A}$ is similar to a regular crossed product $(K/k, c)$ where the order of c divides the exponent of $\mathfrak{A}$. Assume now that the characteristic of k is 0 and that $(K/k, c)$ is a regular crossed product. Denote by $m = m(c)$ the order of c, i.e. the smallest positive integer j such that $c(\sigma, \tau)^j = 1$ for all $\sigma, \tau \in G = G(K/k)$. We are going to construct a set $\mathfrak{R}(K/k, c)$ of isomorphism classes of irreducible continuous representations $R : G_k \to GL(n, \overline{k})$ - where G_k is regarded as a topological group with respect to the profinite topology and $GL(n, \overline{k})$ as a topological group with respect to the discrete topology - under the following assumption.

(1.1) **Assumption** $H^2(G_{k'}, \mathbf{Q}/\mathbf{Z}) = \{0\}$ *for every finite abelian subextension* k'/k *of* $\overline{k}/k$.

It is well known that this assumption holds if k is a local or global number field, see $[T]$ and $[SE1]$, §6; and - of course - it holds if k is a field of cohomological dimension ≤ 1, see $[SE4]$, II, §3, especially 3.3 for examples. In order to construct $\mathfrak{R}(K/k, c)$ we put $G_m := G(K/k(\mu_m))$, $c_m :=$ restriction of c to $G_m \times G_m$; hence $c_m : G_m \times G_m \xrightarrow{c} \mu_m \hookrightarrow k(\mu_m)^*$ is a central 2-cocycle. Let $T : G_m \to GL(n, \overline{k})$ be an irreducible continuous c_m-representation of G_m, comp.$[M]$; so we have $T(\sigma)T(\tau) = c_m(\sigma, \tau)T(\sigma\tau)$ for all $\sigma, \tau \in G_m$. It follows from (1.1) that T has a lifting, i.e. there is a continuous irreducible linear representation $D : G_{k(\mu_m)} \to GL(n, \overline{k})$ such that the corresponding projective representations $\overline{D}$ and $\overline{T}$ coincide, see e.g. $[SE1]$, §6. Denote by $\mathfrak{R}_D$ the set of all isomorphism classes (R) of irreducible continuous linear representations R of G_k of finite degree such that the restriction of R to $G_{k(\mu_m)}$ contains D as an irreducible constitutent, and let $\mathfrak{R}(K/k, c)$ denote the union of all sets $\mathfrak{R}_D$ where D is any linear representation of $G_{k(\mu_m)}$ of finite degree which lifts an irreducible c_m-representation of G_m. Using the Clifford Mackey theory, see $[CL]$ and $[M]$ or the corresponding sections in $[CR]$, one proves the following proposition, for details see $[O3]$, §1.

(1.2) **Proposition** *The degree of every* $(R) \in \mathfrak{R}(K/k, c)$ *divides the degree* $(K : k)$.

§2. Regular crossed products and Galois representations in the case of number fields

Let k be a number field. A continuous linear or projective representation D of G_k over $\overline{k}$ of finite degree is said to be unramified outside a given finite set of places S of k, if for all places of k which do not belong to S the corresponding inertia subgroups are contained in the kernel of D. As is well known, using e.g. the nonabelian version of the "Führerdiskriminantenproduktformel" in $[S2]$,VI, §3, Cor. 2, p. 104, the following result is an easy consequence of a result of I. Schur $[S]$ and a variant of the well known result of Hermite and Minkowski according to which there are only finitely many number fields with a given discriminant, see e.g. $[K]$, Satz 2.13.6, S. 57.

(2.1) **Proposition** *Let* k *be a number field, let* S *be a finite set of places of* k*, let* n *be a positive integer and let* E/k *be a subextension of* $\overline{k}/k$ *of finite degree. Then there are only finitely many isomorphism classes of continuous linear representations* $R : G_k \to GL(n, \overline{k})$ *such that* R *is unramified outside* S *and such that all values of the character of* R *belong to* E*.*

In view of this result it seems worthwhile to investigate rationality and ramification properties of representations of the form constructed above from regular crossed products. For any c.s. k-algebra $\mathfrak{A}$ denote by $S_{\mathfrak{A}}$ the finite set of all places of k at which $\mathfrak{A}$ does not split. Let $(K/k, c)$ be a regular crossed product which is similar to $\mathfrak{A}$. Denote by $S_{K/k}$ the finite set of all places which are ramified in K/k. Since all values of c are roots of unity it follows from the local theory

of central simple algebras, see e.g. $[D]$, VII, §2, especially Satz 3, p.112, that $\mathfrak{A}$ splits at all places which are unramified in K/k. So we have $S_{\mathfrak{A}} \subset S_{K/k}$. It was observed by Hasse $[H]$, see also $[D]$, VII, Satz 4, S. 118, that there is a smallest multiple $g = g(\mathfrak{A})$ of the exponent $\exp(\mathfrak{A})$ of $\mathfrak{A}$ such that $k(\mu_g)$ is a splitting field of $\mathfrak{A}$; namely, by the local theory of c.s. algebras and by the local-global principle for c.s. algebras, see $[D]$, VII, §5, Satz 1, p. 117, g is the smallest positive multiple of the exponent of $\mathfrak{A}$ such that the local degrees $(k_v(\mu_g) : k_v)$ are divisible by $\exp(\mathfrak{A})$ for all $v \in S_{\mathfrak{A}}$. Let $m = m(c)$ denote the order of c. Define the *cyclotomic index* $\widetilde{g} := \widetilde{g}(K/k, c)$ of $(K/k, c)$ by $l.c.m.(m(c), g(\mathfrak{A}))$ if m is odd and by $l.c.m.(4.m(c), g(\mathfrak{A}))$ if m is even. Using the profinite version of the exact Hochschild-Serre sequence, see e.g. $[SH]$,chapter II, §4, and results in $[P]$, section 2, one proves

(2.2) **Proposition** *There is* $(R) \in \mathfrak{R}(K/k, c)$ *such that all values of the character of* R *belong to* $k(\mu_{\exp(G(K/k)).\widetilde{g}(K/k,c)})$.

For every positive integer t denote by S_t the set of all places of k which divide t and the infinite place of $\mathbf{Q}$, and for every finite set of places S of k let k_S/k denote the maximal Galois subextension of $\overline{k}/k$ which is unramified outside S.

(2.3) **Assumption** *Let* q *be a prime number. Then for every finite set of places* S *of* k *which contains* S_q *the following statement holds:*

$L(S, q)$: $H^2(G(k_S/k'), \mathbf{Q}_q/\mathbf{Z}_q) = \{0\}$ *for every finite abelian subextension* k'/k *of* k_S/k.

It is known that $L(S, q)$, which is related to the Leopoldt-conjecture, is true if k is an abelian extension of $\mathbf{Q}$; see $[BR]$ in connection with $[MK]$.

Let $m = q^i$ be a power of a prime number q and let S be a finite set of places of k containing $S_m \cup S_{K/k}$. Then under assumption (2.3) there is a smallest positive integer $\lambda = \lambda(K/k, c)$ such that the central embedding problem for $G(k_S/k(\mu_m))$ which is defined by the cocycle class $(c_m) \in H^2(G_m, \mu_m)$ is weakly solvable with respect to λ, i.e. the central embedding problem for $G(k_S/k(\mu_m))$ corresponding to the image of (c_m) under the homomorphism of cohomology groups with respect to the trivial group action $H^2(G_m, \mu_{q^i}) \to H^2(G_m, \mu_{q^{i+\lambda}})$ which is induced by the embedding $\mu_{q^i} \hookrightarrow \mu_{q^{i+\lambda}}$ is solvable; $l := l(K/k, c) := q^{i+\lambda}$ is called the *Leopoldt-index* of the regular crossed product $(K/k, c)$. A more detailed investigation of closely related invariants is contained in $[NO]$. For any continuous representation R of G_k denote by S_R the set of all places of k which are ramified in the fixed field of the kernel of R.

(2.4) **Proposition** *Under assumption (2.3) there is* $(R) \in \mathfrak{R}(K/k, c)$ *such that* $S_R \subset S_{K/k}$ *and such that all values of the character of* R *belong to* $k(\mu_{\exp(G).l(K/k,c)})$.

§3. Finite symplectic Galois modules and regular crossed products

Let k be a field of characteristic 0 such that assumption (1.1) holds. Let A be a finite continuous G_k-module which is equipped with a nondegenerate symplectic G_k-equivariant pairing $\omega : A \times A \to \mu_m$. It can be shown that there is a central 2-cocycle $f : A \times A \to \mu_m$ such that $\omega(x,y) = f(x,y)/f(y,x)$, $x, y \in A$, and that every cocycle class $(\alpha) \in H^1(G_k, A)$ defines a unique element in the Brauer group $Br(k)$ of k which can be represented by a regular crossed product $(K_{(\alpha)}/k, c)$, where $K_{(\alpha)}$ is a finite Galois splitting field of (α) and $c = c_{(\alpha),f} : G_{(\alpha)} \times G_{(\alpha)} \to \mu_m \subset K^*_{(\alpha)}$ is a Galois 2-cocycle on $G_{(\alpha)} := G(K_{(\alpha)}/k)$ all of whose values belong to μ_m; see [O3], §3. Put $\mathfrak{R}_{(\alpha),f} := \mathfrak{R}(K_{(\alpha)}/k, c)$. Denote by K_A the fixed field of the kernel of the action of G_k on A. We assume

(3.1) $\quad \rho := res^{G_k}_{G_{K_A}}((\alpha)) \in Hom(G_{K_A}, A)^{G(K_A/k)}$ *is surjective.*

It is easily seen that there is $(\alpha) \in H^1(G_k, A)$ satisfying (3.1) provided $H^2(G(K_A/k), A)$ is trivial. In fact, according to [IK] there is a surjective solution ϕ of the embedding problem for G_k which is defined by the semidirect product of the $G(K_A/k)$-module A with $G(K_A/k)$. The restriction of ϕ to G_{K_A} yields a surjective $\rho \in Hom(G_{K_A}, A)^{G(K_A/k)}$. Since $H^2(G(K_A/k), A) = \{1\}$ by assumption, the exact Hochschild-Serre sequence shows that there is $(\alpha) \in H^1(G_k, A)$ such that $\rho = res^{G_k}_{G_{K_A}}((\alpha))$. Examples of symplectic G_k-modules A with trivial $H^2(G(K_A/k), A)$ arise naturally in the theory of elliptic curves; see [SE3]. Representations similar to those in $\mathfrak{R}_{(\alpha),f}$ have been constructed by a different method, which is implicit e.g. in [W], in [O1]. For the algebraic framework see also [Z].

§4. Examples

In this section we describe various examples.

(1) Central pairs and Galois representations, see also [O2], [O3], [O4].

Let k be a field of characteristic 0. Let A be a finite abelian group of prime exponent and let $f : A \times A \to k^*$ be a central 2-cocycle. (A, f) is called a *central pair*. As can be seen from [A],chapter V, section 4, p. 186ff, central pairs arise naturally in the theory of quadratic forms. We assume that (A, f) has the following properties:

(a) The symplectic pairing $\omega_f : A \times A \to k^*$, $\omega_f(x,y) := f(x,y)/f(y,x)$, $x, y \in A$, which was introduced in [IM], §1, p.132, is nondegenerate; so especially all values of ω_f belong to μ_m where m is the exponent of A, and $\mu_m \subset k^*$.

(b) The central pair (A, f) is *full*, which means that the following conditions (i) and (ii) hold:

(i) There is a map $\alpha_f : A \to \overline{k}^*$ such that

$\alpha_f(x)^{ord(x)} = \prod_{j=1}^{ord(x)} f(x, x^j)$ for all $x \in A$

(ii) The degree of every $\alpha_f(x)$, $x \in A$, over k is the order $ord(x)$ of x, and the degree of the extension k_f/k which is generated over k by all $\alpha_f(x)$, $x \in A$, is the order of A.

Then, if we consider A as a trivial G_k-module, the pair (A, ω_f) is a nondegenerate symplectic G_k-module. Moreover, the composition of maps

$$\alpha : G_k \stackrel{\beta}{\to} \widehat{A} \stackrel{\gamma}{\to} A,$$

where

$$\beta(\sigma)(x) := \sigma(\alpha_f(x))/\alpha_f(x) \text{ for all } \sigma \in G_k,\ x \in A,$$

and

$$\gamma(\lambda) := x_\lambda \text{ is such that } \lambda(y) = \omega_f(x_\lambda, y) \text{ for all } \lambda \in \widehat{A},\ y \in A,$$

defines a surjective homomorphism

$$(\alpha) \in H^1(G_k, A) = Hom(G_k, A)$$

with the property $k_{(\alpha)} = k_f$. Let $f_0 : A \times A \to \mu_m$ denote a central 2-cocycle such that $\omega_f = \omega_{f_0}$. Then $\mathfrak{R}_{(\alpha),f_0}$ is defined. This set has been constructed and investigated in [$O2$] . Especially the following results are shown there:

The character group $\widehat{G}_k$ acts transitively on $\mathfrak{R}_{(\alpha),f_0}$. Every $(R) \in \mathfrak{R}_{(\alpha),f_0}$ has degree $|A|^{1/2}$. If k is a number field there is $(R) \in \mathfrak{R}_{(\alpha),f_0}$ such that $S_{(R)} \subset \{v : v \text{ divides } m,\ v \text{ divides } a_f(x) \text{ for all } x \in A,\ v \text{ divides } \infty\}$, and all values of the character of (R) belong to $k(\mu_{\widetilde{g}})$ where $\widetilde{g}$ is the cyclotomic index of (α).

Moreover, as was observed in [$O2$] , the results on automorphic induction in [AC] imply:

For a number field $k \subset \mathbb{C}$ every $(R) \in \mathfrak{R}_{(\alpha),f_0}$ is cuspidal automorphic in the sense of [L] . More precisely the cuspidal automorphic representation corresponding to $(R) \in \mathfrak{R}_{(\alpha),f_0}$ is automorphically induced in the sense of [AC] by a continuous character λ of $GL(1, \mathbb{A}_M)$ of finite order where $M \subset k_f$ is the

fixed field corresponding to any maximal ω-isotropic subgroup of A under the above isomorphism $\alpha : G(k_f/k) \cong A$, and the character λ corresponds under the Artin map $GL(1, \mathbb{A}_M) \to G_M^{ab}$ (see [AT]) to a continuous character $\widetilde{\lambda}$ of G_M such that the restriction of $\widetilde{\lambda}$ to G_{k_f} is the central character γ_R of (R), i.e. γ_R is the unique irreducible constituent of the restriction of R to G_{k_f}.

(Here $\mathbb{A}_K$ denotes the adele ring of the number field K.)

In the special case $A \cong \mathbf{Z}/2 \times \mathbf{Z}/2$ the corresponding modular forms include those constructed by E. Hecke [HE] from indefinite binary quadratic forms, see [$O2$], section 4, and the literature mentioned there; and also certain wave forms, see [$O4$] and the literature mentioned there.

(2) Elliptic curves and Galois representations, see also [BF], [BU], [HA], [J], [$O1$], [$O2$], [$O3$].

Let X be an elliptic curve defined over k. For any positive integer m denote by X_m the kernel of the multiplication by m homomorphism $X(\overline{k}) \stackrel{m}{\to} X(\overline{k})$. The Weil-pairing $\omega = \omega_m : X_m \times X_m \to \mu_m$ is a nondegenerate bilinear G_k-equivariant symplectic pairing, see [T]. Let $f : A \times A \to \mu_m$ be a central 2-cocycle such that $f(x,y)/f(y,x) = \omega(x,y)$, $x, y \in A$. Every k-rational point $P \in X(k) \setminus mX(k)$ defines an element $\Delta(P) \in H^1(G_k, X_m)$, $\Delta(P)(\sigma) := \sigma(Q) - Q$ for all $\sigma \in G_k$, where $Q \in X(\overline{k})$ is such that $mQ = P$. If the restriction $\Delta(P)_{/G_{k(X_m)}} \in Hom(G_{k(X_m)}, X_m)^{G(k(X_m)/k)}$ is surjective, then, according to the above construction, the rational point P defines the set $\mathfrak{R}_{P,f} := \mathfrak{R}_{\delta(\Delta(P)),f}$ of isomorphism classes of continuous irreducible representations of G_k over $\overline{k}$. In the case of number fields Kummer theory for elliptic curves as developed in [BK] and [LG], chapter V, yields examples with surjective $\Delta(P)_{/G_{k(X_m)}}$. Similar representations have been constructed in a slightly different way in [$O1$]. They were investigated further in [J]. The construction of an odd 2-dimensional Galois representation of octahedral type of Artin-conductor 59^2 in [HA] makes also use - at least implicitly - of an elliptic curve, namely $X : y^2 = x^3 + 2x - 1$. The construction and thorough investigation of odd 2-dimensional Galois representations of $G_{\mathbf{Q}}$ of octaedral type in [BF] and [BU] is based on elliptic curves X over $\mathbf{Q}$ and nontrivial elements in $H^1(G_{\mathbf{Q}}, X_2)$ which are interpreted in terms of 2-coverings of X. For the theory of m-coverings of elliptic curves see [BS] and [C].

References

[A] E. Artin: Geometric algebra, Interscience, New York, 1957

[AT] E. Artin, J. Tate: Class field theory, Benjamin, New York, 1967

[AC] J. Arthur, L. Clozel: Simple algebras, base change and the advanced theory of the trace formula, Annals of Mathematics Studies 120, Princeton University Press, New Jersey, 1989

[BK] M.I. Bashmakov: The cohomology of Abelian varieties over a number field, Russian Mathematical Surveys, 27, 1972, 2, 25-70

[B] R. Brauer: Über die Konstruktion der Schiefkörper, die von endlichem Rang in bezug auf ein gegebenes Zentrum sind, JRAM, 168, 1932, 44-64

[BR] A. Brumer: On the units of algebraic number fields, Mathematica, 14, 1967, 121-124

[BF] P. Bayer, G. Frey: Galois representations of octahedral type and 2-coverings of elliptic curves, Mathematische Zeitschrift, 207, 1991, 395-408

[BU] M. Bungert: Konstruktion von Modulformen niedrigen Gewichts, Preprint Serie, Institut für experimentelle Mathematik Essen, 12, 1990

[BS] B.J. Birch, H.P.F. Swinnerton-Dyer: Notes on elliptic curves I, JRAM, 212, 1963, 7-25

[C] J.W.S. Cassels: Diophantine equations with special reference to elliptic curves, J. London Math. Soc., 41, 1966, 193-291

[CL] A.H. Clifford: Representations induced in an invariant subgroup, Annals of Mathematics, 38, 1937, 533-550

[CR] C.W. Curtis, I. Reiner: Representation theory of finite groups and associative algebras, Wiley, New York, 1962

[D] M. Deuring: Algebren, Springer Verlag, Berlin, 1935

[HA] K. Haberland: Perioden von Modulformen einer Variablen und Gruppenkohomologie III, Mathematische Nachrichten, 112, 1983, 297-315

[H] H. Hasse: Die Struktur der R. Brauerschen Algebrenklassengruppe über einem algebraischen Zahlkörper, Math. Ann., 107, 1933, 731-760

[HE] E. Hecke: Über einen Zusammenhang zwischen elliptischen Modulfunktionen und indefiniten quadratischen Formen, in: Mathematische Werke, Vandenhoeck und Ruprecht, Göttingen, 1959, No. 22, 1925, pp.418-427

[IK] M. Ikeda: Zur Existenz eigentlicher galoisscher Körper beim Einbettungsproblem, Abh. Math. Seminar der Univ. Hamburg, 24, 1960, 126-131

[IM] N. Iwahori, H. Matsumoto: Several remarks on projective representations of finite groups, Journal of the Faculty of Science of the University of Tokyo, Sect. I, 10, 1964, 129-146

[J] F. Jonas: Galoisdarstellungen und Einbettungsprobleme mit beschränkter Verzweigung, Dissertation, Universität Göttingen, 1991

[K] H. Koch: Zahlentheorie, Vieweg Verlag, Braunschweig/Wiesbaden, 1997

[LG] S. Lang: Elliptic curves diophantine analysis, Springer, Berlin, 1978

[L] R.P. Langlands: Problems in the theory of automorphic forms, in: Lectures in modern analysis and applications, LNM 170, Springer Verlag, New York, 1970

[M] G. W. Mackey: Unitary representations of group extensions I, Acta Mathematica, 99, 1958, 265-311

[MK] K. Miyake: Leopoldt kernels and central extensions of numbert fields, Nagoya Math. J., 120, 1990, 67-76

[NO] Q. D. Th. Nguyen, H. Opolka: Numerical invariants of central embedding problems, Journal of Number Theory, 52, 1995, 7-16

[$O1$] H. Opolka: Galoisdarstellungen und Galoiskohomologie von Zahlkörpern, Schriftenreihe des Mathematischen Instituts der Universität Münster, 2. Serie, Heft 27, 1983

[$O2$] H. Opolka: Central pairs, Galois theory and automorphic forms, Algebras and Representation Theory, 6, 2003, 449-459

[$O3$] H. Opolka: A note on regular crossed products and Galois representations, Communications in Algebra, Taylor & Francis Group, 35, 2007, 1469-1478

[$O4$] H. Opolka: Composite numbers, Galois theory and automorphic forms, July 2009, Digitale Bibliothek Braunschweig,

http://www.digibib.tu-bs.de/?docid=00028755

[P] G. Poitou: Conditions globales pour des problèmes de plongement à noyau abélien, Annales de L'Institut Fourier, XXIX, 1979, 1-14

[S] I. Schur: Über eine Klasse von endlichen Gruppen linearer Substitutionen, Nr. 6 der Ges. Abh., Springer Verlag, Berlin, 1973

[$SE1$] J.P. Serre: Modular forms of weight one and Galois representations, in: A. Fröhlich (ed.): Algebraic number fields, Academic Press, New York, 1977, pp. 193-268

[$SE2$] J.P. Serre: Local fields, Springer Verlag, New York, 1979

[$SE3$] J.P. Serre: Propriete galoisiennes des points d'ordre fini des courbes elliptiques, Inventiones Mathematicae, 15, 1972, 259-331

[$SE4$] J. P. Serre: Galois cohomology, Springer Verlag, Berlin, 1997

[SH] S.S. Shatz: Profinite groups, arithmetic and geometry, Annals of Mathematics Studies, Princeton University Press, 1972

[T] J. Tate: Duality theorems in Galois cohomology over number fields, Proceedings of the International Congress of Mathematicians, Stockholm, 1962, 288-295

[W] A. Weil: Sur certains groupes d'operateurs unitaires, Acta Mathematica, 111, 1964, 143-211

[Z] E. W. Zink: Weil Darstellungen und lokale Galoistheorie, Mathematische Nachrichten, 92, 1979, 265-288

Typeset with Scientific Word and LaTex